Cryptanalysis of quantum broadcast communication and authentication protocol with a one-time pad*

Ya Cao(曹雅)[1,2] and Fei Gao(高飞)[1,†]

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] State Key Laboratory of Cryptology, Beijing 100878, China

(Received 23 May 2016; revised manuscript received 7 July 2016; published online 30 September 2016)

Chang *et al.* [*Chin. Phys. B* **23** 010305 (2014)] have proposed a quantum broadcast communication and authentication protocol. However, we find that an intercept-resend attack can be preformed successfully by a potential eavesdropper, who will be able to destroy the authentication function. Afterwards, he or she can acquire the secret transmitted message or even modify it while escaping detection, by implementing an efficient man-in-the-middle attack. Furthermore, we show a simple scheme to defend this attack, that is, applying non-reusable identity strings.

Keywords: quantum broadcast communication, quantum secure direct communication, Greenberger–Horne–Zeilinger (GHZ) state, authentication

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a, 03.65.Ud **DOI:** 10.1088/1674-1056/25/11/110305

1. Introduction

Cryptography aims at sharing secret messages between users, while revealing nothing to eavesdroppers. In classical cryptography, most schemes are conditionally secure under the assumption of computational complexity, except for the one-time pad (OTP) crypto-system. In OTP, an unconditional secure string is used to encrypt messages to be transmitted in a public way. The major difficulty of the OTP crypto-system comes from how to securely distribute key bits. Quantum key distribution (QKD) is such a mechanism to transfer an unconditional secure string. Since the first QKD protocol was proposed by Bennett and Brassard in 1984,[1] QKD has attracted a great deal of attention because of its attractive property of being unconditionally secure, and a lot of QKD protocols have been presented.[2–9] Besides QKD, a variety of quantum cryptography has been proposed, such as quantum secret sharing (QSS),[10–13] quantum signature (QS),[14–17] and quantum private queries (QPQ).[18–24] In the last few years, QPQ has become a subject of intense focus. It solves the most concerned problem of privacy of both database and users, which still needs to be further studied.

Recently, quantum secure direct communication (QSDC) appeared as a novel branch of QKD.[25–40] Different from QKD, QSDC is to realize the task of transmitting messages directly, without pre-shared secret keys. The first QSDC was presented by Beige *et al.* with a single photon in 2001.[25] In 2002, Boström and Felbinger put forward a ping-pong scheme with Einstein–Podolsky–Rosen (EPR) pairs.[26] However, the ping–pong scheme is proved to be quasisecure when using a perfect quantum channel.[27] Later, in order to improve the security, Deng *et al.* presented a two-step QSDC scheme.[28] In their paper, a sequence of ordered EPR pairs is prepared and then divided into two subsequences, where one serves as the checking string and the other as the message-encoding string. In 2004, Deng and Long presented a QSDC scheme with a one-time pad crypto-system which is more practical.[29] Thereafter, the investigation into multiparty QSDC schemes has naturally been considered.[41]

Quantum broadcast communication (QBC)[41–43] is one kind of multiparty QSDC scheme. QBC is a scheme which attempts to transmit secret messages from the sender Alice to a dynamically changing group of users (Bob, Charlie, ...) through broadcasting channels. QBC ensures only authorized users obtain subscribed information and others can learn nothing. In 2007, Wang *et al.* proposed three QBC schemes, where identity authentication is realized by utilizing hash function and local unitary operations.[42] Later in 2010, Yang *et al.* improved the scheme of Wang *et al.* in efficiency, and also used the hash function to authenticate identity.[43] It is known that design is an important work in cryptography. As pointed out by Lo and Ko, breaking cryptographic systems was as important as building them.[44] Cryptanalysis is also important for quantum cryptography.[45–50] It helps estimate the security of a protocol, find potential loopholes in it, and improve it to level up the security.

More recently, Chang *et al.* proposed a quantum broadcast communication and authentication (QBCA) protocol,[51] based on the Greenberger–Horne–Zeilinger (GHZ) state and a one-time pad crypto-system. This protocol is easier to be implemented than that referred to by Wang *et al.*[42] and Yang *et al.*[43] The reason is that Chang *et al.*'s protocol gives up

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61272057 and 61170270).
†Corresponding author. E-mail: caoshinee@126.com
© 2016 Chinese Physical Society and IOP Publishing Ltd

hash functions and local unitary operations for eavesdropping detection and authentication, but applies a reusable pre-shared binary string serving as an identity string, and the classical XOR operation. However, the security requirements may not be satisfied as mentioned in Chang *et al.*'s protocol.

In this paper, we study and analyze the security of Chang *et al.*'s QBCA protocol. We implement a devised intercept-resend attack, which introduces no error. By applying this attack, a potential eavesdropper Eve can successfully deduce the identity strings, which are the symbols of authorized users. With these identity strings, Eve has the capacity to implement an efficient man-in-the-middle attack.[56] That is to say, Eve can impersonate an authorized user to communicate with the sender and obtain the transmitted message, or the sender to transfer the transmitted message or even a modified one (e.g., a useless message) to authorized users, while not being detected. To avoid this loophole, we also put forward a possible manner to help suffer the intercept-resend attack.

The rest of this paper is arranged as follows. In Section 2, we review Chang *et al.*'s QBCA protocol in detail. In Section 3, we introduce a devised intercept-resend attack for Chang *et al.*'s protocol and give an improved scheme to avoid the weakness and an analysis to prove it to be effective. Finally, we conclude this paper.

2. Review of Chang *et al.*'s protocol

In this section, we review Chang *et al.*'s protocol. Before the scheme starts, there are some assumptions. Suppose Alice is the sender, and Bob and Charlie are the two legitimate receivers. The secret message to be transmitted is a classical string. Alice pre-shares an N-bit identity string $\mathrm{ID_B}$ and $\mathrm{ID_C}$ with Bob and Charlie, respectively. The details of Chang *et al.*'s scheme are described below.

Step 1 Alice generates three sequences of quantum states, one serving as the information carrier, and the other two as decoy states. Firstly, she prepares a sequence of ordered N triplet GHZ states in the form $|\phi>=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{123}$. She then divides the N GHZ states into three ordered particle sequences S_1, S_2 and S_3, respectively, where the subscript indicates which sequence each particle of every state belongs to. After that, she prepares N-qubit sequences S_{IDB} and S_{IDC} according to $\mathrm{ID_B}$ and $\mathrm{ID_C}$, respectively. Taking S_{IDB} as an example, if the i-th bit of $\mathrm{ID_B}$ (denoted as $\mathrm{ID_B}^i$) is 0, S^i_{IDB} is randomly encrypted by qubit $|0\rangle$ or $|1\rangle$; otherwise, S^i_{IDB} is randomly encrypted in state $|+\rangle$ or $|-\rangle$. S_{IDC} is prepared in the same way.

Step 2 Alice inserts S_{IDB} and S_{IDC} into S_2 and S_3, constructing new sequences S'_2 and S'_3, respectively. Concretely, if $\mathrm{ID_B}^i=0$, Alice inserts S^i_{IDB} behind S^i_2; otherwise, she inserts it before S^i_2. She constructs S'_3 with the same method. Then Alice transmits S'_2 and S'_3 to Bob and Charlie, respectively.

Step 3 Bob and Charlie distinguish S_{IDB} and S_{IDC} from S'_2 and S'_3 with the knowledge of $\mathrm{ID_B}$ and $\mathrm{ID_C}$, respectively. Then they both measure S_{IDB} and S_{IDC} with corresponding bases of S_{IDB} and S_{IDC}.

Step 4 Alice requires Bob and Charlie to declare the state of each photon in S_{IDB} and S_{IDC}, but not including the basis information. One possible way for Bob and Charlie is to publish bit 0 for the result $|0\rangle$ or $|+\rangle$, and 1 for $|1\rangle$ or $|-\rangle$. Then Alice authenticates them by comparing the announced information with the initial states of S_{IDB} and S_{IDC}. If the error rates are low enough, Alice confirms Bob and Charlie are legitimate users and believes there are no eavesdroppers. Then they proceed to the next step. Otherwise, Alice stops this communication.

Step 5 Bob and Charlie use the Z basis to measure every photon in S_2 and S_3, forming ordered classical sequences C_{S_2} and C_{S_3}, respectively. Bob and Charlie both announce which photons they do not receive in S_2 and S_3 in order. For lost photons, Alice discards corresponding photons in S_1, so do Bob and Charlie. Then Alice measures the remaining photons in S_1 with Z basis forming an ordered classical sequence C_{S_1}. Suppose C_{S_1} is an N_1-bit string. Alice takes the first N_1 bit from secret message M as M_1, and encrypts it with C_{S_1} using the XOR operation bit by bit to obtain encrypted message C. Then Alice publishes C.

Step 6 Bob and Charlie decrypt C with C_{S_2} and C_{S_3}, respectively, using XOR operation bit by bit, then obtain secret message M_1 and store it. Till now, Alice, Bob, and Charlie complete one communication.

3. Analysis and improvement

3.1. Security analysis of Chang *et al.*'s QBCA protocol

In Chang *et al.*'s QBCA protocol, the authors have proved the security based on the fact that the true random number C_{S_1} used as a one-time pad is unknown to anyone else except Alice and Bob. Suppose an eavesdropper Eve, who does not know the number C_{S_1}, tries to obtain the transferred message, she will fail since the OTP is a secure system. However, is it true that Eve really cannot get the number C_{S_1}? To answer the question, we should first track the security foundation of the number C_{S_1}. C_{S_1} is formed by measuring sequence S_1 with the Z basis in order. A legal user Bob can deduce C_{S_1} from S_2. The security of S_2 comes from the secure positions of the bits in S_2 or S_{IDB}, and identity string S_{IDB} determines the positions. However, in Chang *et al.*'s QBCA protocol, Bob's identity S_{IDB} will be totally leaked out to Eve. The chance is given by that the identity string is reusable. Afterwards, we will prove it in detail.

We first introduce an intercept-resend attack to Chang *et al.*'s protocol to invalidate the authentication function and then implement a successful man-in-the-middle attack to ob-

tain the transmitted message or even replace it with a modified one. It is obvious that, in Chang *et al.*'s protocol, the authorized users Bob and Charlie act in the same character to the sender Alice, and behave the same in the protocol. Without loss of generality, we take Bob as an example to analyze Chang *et al.*'s protocol.

Reviewing Chang *et al.*'s QBCA protocol, we find that the test for the authentication is also a test for potential eavesdroppers. Both processes functioning wells are due to the fact that just Alice and Bob know the pre-shared identity string. Without the identity $\mathrm{ID_B}$, an eavesdropper Eve cannot successfully cheat Alice to obtain the secret message. Since she does not know $\mathrm{ID_B}$, she cannot provide the proper information in Step 4, so Alice will calculate a high error rate and then detect Eve. However, in Chang *et al.*'s protocol, the identity string will be totally revealed. This is because of the statement that the identity string is reusable. By exploiting this little defect, we present an effective attack on Chang *et al.*'s protocol.

Eve attacks Chang *et al.*'s protocol using the following steps:

(A1) Eve enters the communication process. She impersonates one participant to contact with the other one, in order to excite the communication.

(A2) Once the communication starts, Eve intercepts every photon from Alice. Then she makes different movements to these photons, according to their positions in the sequence S_2'. If the photon is the $2i$-th qubit of S_2', Eve measures it with the Z basis and resends it to Bob; otherwise, the photon is the $(2i+1)$-th qubit, and she just lets it go towards Bob. Here, i ranges from 1 to N.

(A3) Eve reveals the complete identity string $\mathrm{ID_B}$. When Chang *et al.*'s protocol proceeds to Step 4: the authentication and eavesdropping detection, Eve compares her measurement results with Bob's announcement in order. Repeating this action for enough communications, she is able to obtain $\mathrm{ID_B}$, while not being detected by Alice.

Looking at Step 4 again, we find that, in S_2', the secret qubit and decoy qubit always appear in pairs. That is, one of the $(2i-1)$-th and $2i$-th qubits in S_2' must belong to S_2 and the other belongs to S_{IDB}. Thus, every photon in the even position of S_2' is either a secret qubit or a decoy state corresponding to ${\mathrm{ID_B}}^i = 0$. Another important point in Chang *et al.*'s authentication process lies in that Bob is asked to measure S_{IDB} with the Z basis when ${\mathrm{ID_B}}^i = 0$, as described in Step 4. However, secret photons should also be measured in the Z basis referring to Step 5. These two points ensure that Eve's measurement does not disturb the process where Alice authenticates Bob.

Recalling Chang *et al.*'s protocol, they claimed that the legitimate receiver's identity is a reusable classical string. That is, no matter how many times the protocol runs, Bob always use the same binary string $\mathrm{ID_B}$ for authentication. Therefore, Eve can compare his results in many communications with Bob's publication. As discussed above, for every even photon in S_2', it might be a secret photon, then Eve's measurement result will be equal to what Bob announces with probability $1/2$; otherwise, it is a decoy photon whose corresponding bit in $\mathrm{ID_B}$ is 0, then Eve's result is always the same as Bob's announcement. In ideal circumstances, as long as Eve finds there is one time that his measurement result is unequal to Bob's announcement for the corresponding qubit in S_{IDB}, he can confirm that the i-th identity bit ${\mathrm{ID_B}}^i$ is 1; if Eve's measurement result is always equal to Bob's corresponding announcement many times, he can believe ${\mathrm{ID_B}}^i$ is 0. In the later case, there are two situations for Eve and Bob to have equal results. However, the probability for the case that ${\mathrm{ID_B}}^i = 1$ and induces the same results for n-times communications is $(1/2)^n$, which will be smaller than 10^{-5} if $n = 17$. Hence, if there are enough times when the same results appear, Eve can confirm that ${\mathrm{ID_B}}^i$ is 0.

(A4) Finally, Eve obtains or modifies the secret message by implementing a man-in-the-middle attack.

After the step above, Eve holds the complete identity. When another communication happens, Eve launches it and two protocols are performed in parallel: one is between Alice and Eve, the other is between Eve and Bob. In the former one, Eve poses as a legitimate user. She just executes the protocol normally and the authentication will be passed since she holds the right identity of Bob. In the latter one, Eve acts as the sender. She prepares the necessary qubits to form a fake S_2, called S_2^{E}, sends it to Bob, and passes the authentication. In this way, Eve achieves the man-in-the-middle attack on Chang *et al.*'s protocol. If Eve just wants to acquire the secret message without modifying it, an intercept-resend attack is enough. She first intercepts every photon transmitted by Alice. Then, Eve distinguishes which photon is from S_2, and which one is from S_{IDB}. If the photon comes from S_{IDB}, she just lets it go. Otherwise, she measures it with the Z basis, and then sends it to Bob. Since Eve does nothing to the decoy states, the detection is not disturbed. So Alice's test will be passed. On the other hand, C_{S_2}, which decrypts the secret message, is constructed by measuring S_2 with the Z basis. So Eve's measurement will then reveal the secret message M.

As a result, we successfully make our intercept-resend attack on Chang *et al.*'s protocol. With this attack, Eve acquires the secret identity string S_{IDB}, while introducing no error. On the one hand, she can obtain the secret message which is transferred to authorized user Bob. On the other hand, she will not be detected by the sender Alice. Moreover, by implementing a man-in-the-middle attack, she can impersonate Alice and send Bob a fake message instead of the right one, but Bob will be unaware of it. As mentioned earlier, if we substitute Charlie for Bob in the above process, the analysis and results will be

all the same. Furthermore, since Chang *et al.*'s protocol can be generalized to a multi-party one, our attack also works on the generalized one.

3.2. Improvement of Chang *et al.*'s protocol

Now we consider how to improve Chang *et al.*'s protocol. As we have emphasized, the reason why Chang *et al.*'s protocol is fragile lies in that the identity string is claimed to be reusable. This gives an eavesdropper Eve a chance to play the intercept-resend attack successfully and obtain the secret identities. To plug this loophole, the sender should not pre-share a reusable identity with the user. We modify the protocol as follows.

(R1) Before the protocol starts, we made a substituted supposition that Alice pre-shares an identity store IDB $=\{\mathrm{ID}_{\mathrm{B}1},\mathrm{ID}_{\mathrm{B}2},\ldots\}$, with Bob and IDC $=\{\mathrm{ID}_{\mathrm{C}1},\mathrm{ID}_{\mathrm{C}2},\ldots\}$ with Charlie. Here, each element from IDB and IDC is a string encoded Bob's and Charlie's identity, respectively. They fix a rule to decide the order where these identities are to be used.

The simplest rule is that they agreed to use the identity in order. That is to say, in round 1, Alice uses $\mathrm{ID}_{\mathrm{B}1}$ to run the protocol with Bob, and $\mathrm{ID}_{\mathrm{C}1}$ with Charlie, and Bob and Charlie choose $\mathrm{ID}_{\mathrm{B}1}$ and $\mathrm{ID}_{\mathrm{C}1}$, respectively; in round 2, Alice picks $\mathrm{ID}_{\mathrm{B}2}$ and $\mathrm{ID}_{\mathrm{C}2}$. Meanwhile, Bob uses $\mathrm{ID}_{\mathrm{B}2}$, and Charlie uses $\mathrm{ID}_{\mathrm{C}2}$; etc. They also can make the rule more complex by applying a hash function. A possible way is that Alice, Bob, and Charlie share the same hash function H. They count the run number x, and pick the $H(x)$-th identity, respectively.

(R2) When the protocol begins, Alice picks out identities $\mathrm{ID}_{\mathrm{B}i}$ and $\mathrm{ID}_{\mathrm{C}i}$ from the identity stores according to the agreed rule, and Bob and Charlie choose the corresponding identity, respectively.

The following steps in Chang *et al.*'s protocol are not necessary to be amended. With our strategy, the modified version is able to suffer from the presented intercept-resend attack. In our scheme, we abandon the reusable identity, but utilize a non-reusable identity store. As we have analyzed before, an eavesdropper Eve cannot deduce one bit of the identity if she gets the same result to what Bob announced, for the reason that she is not sure whether this bit corresponds to a qubit from S_{IDB} or S_2. However, this bit is certainly from S_{IDB} corresponding to an identity bit 1, when Eve finds her result is different from that of Bob. On the one hand, for one communication, it is obvious that this attack cannot reveal the complete identity. On the other hand, one may consider whether he can do more with this imcomplete identity or not. However, as pointed out in the Ref. [34], it is not sufficient for him to perform a man-in-the-middle attack or generate fake photons. Furthermore, we update the identity in each communication, so the revealed identity information cannot provide efficient information for the next communication. Thus comparing results from multi-communications is also not an available way for Eve to attack this modified version. Therefore, the modified protocol with non-reusable identity is successful.

To illustrate our analysis in more detail, we make a comparison between the reusable version and the modified one about the information leakage by giving an example. Considering Bob, the simplest case is that there are only two identity strings in IDB, $\mathrm{ID}_{\mathrm{B}1}$ and $\mathrm{ID}_{\mathrm{B}2}$. However, the protocol with a reusable identity just has $\mathrm{ID}_{\mathrm{B}1}$. Suppose each identity concludes one bit, and let $\mathrm{ID}_{\mathrm{B}1}=1$ and $\mathrm{ID}_{\mathrm{B}2}=0$. As shown in Table 1, the probability for the modified version to leak a bit is 1/4; however, this probability is 1/2 in the reusable one.

Table 1. Comparison between reusable and non-reusable version. ID denotes the corresponding bit of $\mathrm{ID}_{\mathrm{B}1}$ and $\mathrm{ID}_{\mathrm{B}2}$. PM-$S_2'$ represents the possible states of S_2' after Eve's and Bob's measurement.

ID	Result	PM-S_2'			
		$\|+\rangle\otimes\|0\rangle$	$\|+\rangle\otimes\|1\rangle$	$\|-\rangle\otimes\|0\rangle$	$\|-\rangle\otimes\|0\rangle$
1	Bob's result	0	0	1	1
	Eve's result	0	1	0	0
		$\|0\rangle\otimes\|0\rangle$	$\|0\rangle\otimes\|1\rangle$	$\|1\rangle\otimes\|0\rangle$	$\|1\rangle\otimes\|1\rangle$
0	Bob's result	0	1	0	1
	Bob's result	0	1	0	1

4. Conclusion

In this paper, we have pointed out that there is a loophole in Chang *et al.*'s QBCA protocol, where an eavesdropper can impersonate any legitimate participants in communication and not be detected. Eve first obtains the secret identity strings of legitimate receivers through an intercept-resend attack without being detected. Then she is able to obtain or modify the transmitted message by impersonating both the sender and legitimate receivers, while not disturbing the protocol. Besides, we present a simple strategy to avoid this loophole by sharing secret identity stores between the sender and authorized users. The security analysis shows the improved scheme is capable of surviving this intercept-resend attack. This makes the improved one more secure.

References

[1] Bennett C H and Brassard G 1984 *Pro. IEEE Int. Conf. on Computers, Systems and Signal Processing* (New York: IEEE) p. 175
[2] Sun Y and Wen Q Y 2010 *Phys. Rev. A* **82** 052318
[3] Wang C Z, Guo H, Ren J G, Cao Y, Peng C Z and Liu W Y 2014 *Science China Physics, Mechanics and Astronomy* **57** 1233
[4] Lu X M, Zhang L J, Wang Y G, ChenW, Huang D J, Li D, Wang S, He D Y, Yin Z Q, Zhou Y, Hui C and Han Z F 2015 *Science China Physics, Mechanics and Astronomy* **58** 120301
[5] Li Y, Bao W S, Li H W, Zhou C and W Y 2015 *Chin. Phys. B* **24** 110307
[6] Wang L, Zhao S M, Gong L Y and Cheng W W 2015 *Chin. Phys. B* **24** 120307
[7] Li Y, Bao W S, Li H W, Zhou C and W Y 2015 *Chin. Phys. B* **25** 10305
[8] An X B, Yin Z Q and Han Z F 2015 *Acta Phys. Sin.* **64** 140303 (in Chinese)
[9] Sun Y, Zhao S H and Dong C 2015 *Acta Phys. Sin.* **64** 140304 (in Chinese)
[10] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev. A* **72** 044302 (in Chinese)
[11] Qin S J, Gao F, Wen Q Y and Zhu F C 2006 *Phys. Lett. A* **357** 101 (in Chinese)

[12] Yang Y G, Chai H P, Wang Y, Teng Y W and Wen Q Y 2011 *Science China Physics, Mechanics and Astronomy* **54** 1619
[13] Sun Y, Gao F, Yuan Z, Li Y B and Wen Q Y 2012 *Quantum Information Processing* **11** 1741
[14] Choi J W, Chang K Y and Hong D 2011 *Phys. Rev. A* **84** 062330
[15] Zhang K J, Song T T, Zuo H J and Zhang W W 2013 *Physica Scripta* **87** 045012
[16] Yu C H, Guo G D and Lin S 2014 *Science China Physics, Mechanics and Astronomy* **57** 2079
[17] Wang T Y, Cai X Q, Ren Y L and Zhang R L 2015 *Sci. Rep.* **5** 9231
[18] Gao F, Liu B, Wen Q Y and Chen H 2012 *Opt. Commun.* **20** 17411
[19] Zhang J L, Guo F Z, Gao F, Liu B and Wen Q Y 2013 *Phys. Rev. A* **88** 022334
[20] Wei C Y, Gao F, Wen Q Y and Wang T Y 2014 *Sci. Rep.* **4** 7537
[21] Yang Y G, Sun S J, Xu P and Tian J 2014 *Quantum Information Processing* **13** 805
[22] Gao F, Liu B, Huang W and Wen Q Y 2015 *IEEE Journal of Selected Topics in Quantum Electronics* **21** 98
[23] Liu B, Gao F, Huang W and Wen Q Y 2015 *Science China Physics, Mechanics and Astronomy* **58** 100301
[24] Wei C Y, Wang T Y and Gao F 2016 *Phys. Rev. A* **93** 042318
[25] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2002 *Journal of Physics A: Mathematical and General* **35** L407
[26] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[27] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901
[28] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[29] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[30] Zhang Z J, Liu J, Wang D and Shi S H 2007 *Phys. Rev. A* **75** 026301
[31] Lin S, Wen Q Y, Gao F and Zhu F C 2008 *Phys. Rev. A* **78** 064304
[32] Qin S J, Wen Q Y, Meng L M and Zhu F C 2009 *Science in China Series G: Physics, Mechanics and Astronomy* **52** 1208
[33] Liu D, Pei C X, Quan D X and Zhao N 2010 *Chin. Phys. Lett.* **27** 050306
[34] Gao F, Qin S J, Guo F Z and Wen Q Y 2011 *Chin. Phys. Lett.* **28** 020303
[35] Huang W, Wen Q Y, Jia H Y, Qin S J and Gao F 2012 *Chin. Phys. B* **21** 100308
[36] Chang Y, Xu C, Zhang S and Yan L 2014 *Chin. Sci. Bull.* **59** 2541
[37] Zou X F and Qiu D W 2014 *Science China Physics, Mechanics and Astronomy* **57** 1696
[38] Zawadzki P 2015 *Quantum Information Processing* **14** 2589
[39] Ma H Y, Qin G Q, Fan X K and Chu P C 2015 *Acta Phys. Sin.* **64** 160306 (in Chinese)
[40] Li X H 2015 *Acta Phys. Sin.* **64** 160307 (in Chinese)
[41] Deng F G, Long G L, Wang Y and Xiao L 2004 *Chin. Phys. Lett.* **21** 2097
[42] Wang J, Zhang Q and Tang C J 2007 *Chin. Phys.* **16** 1868
[43] Yang Y G, Wang Y H and Wen Q Y 2010 *Chin. Phys. B* **19** 070304
[44] Lo H and Ko T 2005 *Quantum Information Processing* **5** 41
[45] Deng F G, Li X H, Zhou H Y and Zhang Z j 2005 *Phys. Rev. A* **72** 044302
[46] Gao F, Guo F Z, Wen Q Y and Zhu F C 2005 *Phys. Rev. A* **72** 036302
[47] Qin S J, Gao F, Wen Q Y and Zhu F C 2007 *Phys. Rev. A* **76** 062324
[48] Gao F, Qin S J, Guo F Z and Wen Q Y 2011 *Phys. Rev. A* **84** 022344
[49] Wang T Y and Li Y P 2013 *Quantum Information Processing* **12** 1991
[50] Huang W, Yang Y H and Jia H Y 2015 *Quantum Information Processing* **14** 2211
[51] Chang Y, Xu C X, Zhang S B and Yan L L 2014 *Chin. Phys. B* **23** 010305
[52] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049
[53] Deng F G, Li X H, Li C Y, Zhou P, Liang Y J and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 1676
[54] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys. Lett.* **24** 23
[55] Zheng C and Long G F 2014 *Science China Physics, Mechanics and Astronomy* **57** 1238
[56] Lin T H and Hwang T 2014 *Quantum Information Processing* **13** 917